Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 13 (2007) 1096–1116

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

On the ranks of bent functions ☆

Guobiao Weng, Rongquan Feng *, Weisheng Qiu

LMAM, School of Mathematical Sciences, Peking University, Beijing 100871, PR China

Received 21 February 2006; revised 10 August 2006

Available online 28 March 2007

Communicated by Igor Shparlinski

Abstract

The rank of a bent function is the 2-rank of the associated symmetric 2-design. In this paper, it is shown that it is an invariant under the equivalence relation among bent functions. Some upper and lower bounds of ranks of general bent functions, Maiorana–McFarland bent functions and Desarguesian partial spread bent functions are given. As a consequence, it is proved that almost every Desarguesian partial spread bent function is not equivalent to any Maiorana–McFarland bent function.

Keywords: p-Rank; Bent function; Difference set

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power, and let $\mathbb{F}_q^n$ be the n-dimensional vector space over $\mathbb{F}_q$. Bent functions are Boolean functions from $\mathbb{F}_2^{2t}$ to $\mathbb{F}_2$ whose Fourier coefficients have constant magnitude. They play an important role in coding theory, cryptography and other areas. There are thousands of papers discussing the constructions, properties and applications of bent functions from the last thirty years. However, there are few results on the classification of bent functions.

Two bent functions f and g from $\mathbb{F}_2^{2t}$ to $\mathbb{F}_2$ are equivalent if $g(x) = f(\sigma(x) + \beta) + \ell(x)$ for an automorphism $\sigma \in \mathrm{Aut}(\mathbb{F}_2^{2t}, +)$, an element $\beta \in \mathbb{F}_2^{2t}$, and an affine function ℓ from $\mathbb{F}_2^{2t}$ to $\mathbb{F}_2$.

☆ Supported by NSF of China (10331030, 10571005, 60473019), by 863 Project (No. 2006AA01Z434) and by NKBRPC (2004CB318000).

* Corresponding author.

E-mail addresses: fireblbl@math.pku.edu.cn (G. Weng), fengrq@math.pku.edu.cn (R. Feng), qiuws@pku.edu.cn (W. Qiu).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2007.03.001

Hou [13] found an invariant of equivalent bent functions under the action of general linear groups, and determined all cubic bent functions in eight variables. Dobbertin and Leander [11] reported the recent results in the study of normality and non-normality of bent functions. By discussing the full automorphism groups of bent functions, Dempwolff [7] got some results on the classification of bent functions. In this paper, we define the rank of a bent function, which is an invariant under the equivalence relation among bent functions, and distinguish bent functions by calculating their ranks. We get some upper and lower bounds of ranks of Maiorana–McFarland bent functions and Desarguesian partial spread bent functions. As a consequence, we prove that almost every Desarguesian partial spread bent function is not equivalent to any Maiorana–McFarland bent function. Also we give a bent function which is not equivalent to any Maiorana–McFarland function nor to any Desarguesian partial spread bent function.

This paper is organized as follows. In Section 2, some preliminaries of designs and bent functions are given. In Section 3, the rank of a bent function is defined and some properties are outlined. In Sections 4 and 5, the ranks of Maiorana–McFarland bent functions and those of the Desarguesian partial spread functions are discussed. In the last section, the conclusion and further discussions are given.

2. Preliminaries

Let $\mathcal{D} = (P, \mathcal{B})$ be a (v, k, λ) *design*, where $P = \{p_1, p_2, \ldots, p_v\}$ and $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$ are the sets of *points* and *blocks* of $\mathcal{D}$, respectively; *i.e.*, every block B_i, $1 \leqslant i \leqslant b$, is a k-subset of P, and every pair (p_i, p_j) of points occurs exactly in λ blocks. The design $\mathcal{D}$ is called *symmetric* if $b = v$. The *incidence matrix* of $\mathcal{D}$ is the $b \times v$ matrix $A = (a_{ij})$ whose rows are indexed by the blocks and whose columns are indexed by the points, and whose entry a_{ij} is 1 if $p_j \in B_i$ and 0 otherwise. Let $\mathcal{D}_1 = (P_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (P_2, \mathcal{B}_2)$ be two (v, k, λ) designs, and let A_1 and A_2 be the incidence matrices of $\mathcal{D}_1$ and $\mathcal{D}_2$, respectively. Then $\mathcal{D}_1$ and $\mathcal{D}_2$ are *isomorphic* if there exist permutation matrices U and V such that $UA_1V = A_2$. The *p-rank* of the design $\mathcal{D}$, denoted by $\operatorname{rank}_p(\mathcal{D})$, is defined to be the rank of its incidence matrix A over a field F of characteristic p. Thus isomorphic designs have the same p-rank for any prime p. For more material on designs, we refer the reader to [3,15].

Let G be an abelian group of order v. A (v, k, λ)-*difference set* in G is a k-subset $D \subseteq G$ such that each nonzero $g \in G$ appears exactly λ times in the multiset $\{x - y \mid x, y \in D\}$ of differences from D. It is well known that if D is a (v, k, λ)-difference set in G then we have an associated symmetric (v, k, λ) design $\mathcal{D} = (P, \mathcal{B})$, where $P = G$ and $\mathcal{B} = \{g + D \mid g \in G\}$. The *p-rank* of a difference set D, $\operatorname{rank}_p(D)$, is defined to be the p-rank of its associated symmetric design. Let D_1 and D_2 be two (v, k, λ)-difference sets in an abelian group G. Then D_1 and D_2 are *equivalent* if there exist $\sigma \in \operatorname{Aut}(G)$ and $g \in G$ such that

$$D_1 = g + \sigma(D_2) = \{g + \sigma(d) \mid d \in D_2\}.$$

It is clear that if D_1 and D_2 are equivalent, then their associated designs are isomorphic. Thus equivalent difference sets have the same p-rank for any prime p. So p-rank is helpful to distinguish inequivalent difference sets. For two difference sets D_1, D_2 in G with the same parameters (v, k, λ), we usually prove that D_1 and D_2 are not equivalent by showing $\operatorname{rank}_p(D_1) \neq \operatorname{rank}_p(D_2)$ for some prime p. See Arasu [1] and Chandler and Xiang [5,6] for details.

Two general results on p-ranks of symmetric designs are collected in the following theorems.

Theorem 2.1. *(See [2].) Let $\mathcal{D}$ be a symmetric (v, k, λ) design with order $n = k - \lambda$. Let p be a prime such that $p \nmid n$. Then* $\operatorname{rank}_p(\mathcal{D}) \geqslant v - 1$ *with equality if and only if $p \mid k$.*

Theorem 2.2. *(See [14].) Let $\mathcal{D}$ be a symmetric (v, k, λ) design with order $n = k - \lambda$. Let p be a prime with $p \mid n$. Then* $\operatorname{rank}_p(\mathcal{D}) \leqslant (v + 1)/2$. *Moreover, if $p \nmid \lambda$ and $p^2 \nmid n$, then* $\operatorname{rank}_p(\mathcal{D}) \geqslant v/2$.

From above theorems, the p-rank of a symmetric design depends only on its parameters when $p \nmid n$ or $p \parallel n$ and $p \nmid \lambda$. Things are much different when $p^2 \mid n$ or $p \mid n$ and $p \mid \lambda$. It is interesting and also more difficult to determine the p-ranks of symmetric designs in those cases.

Next we give some preliminaries on bent functions. Let k be an integer. A map $f : \mathbb{F}_2^k \to \mathbb{F}_2$ is called a *bent function* if the Fourier coefficient

$$F(y) = 2^{-k/2} \sum_{x \in \mathbb{F}_2^k} (-1)^{f(x) + x \cdot y}$$

has constant magnitude 1 for all $y \in \mathbb{F}_2^k$, where "$\cdot$" is the usual dot product, i.e.,

$$(x_1, x_2, \ldots, x_k) \cdot (y_1, y_2, \ldots, y_k) = \sum_{i=1}^{k} x_i y_i.$$

It is easy to show that the function $\log F(y)$, where $\log 1 = 0$ and $\log(-1) = 1$, is a bent function on the dual space. This function is called the *dual* of f.

The following characterization of bent functions is from Wolfmann [18].

Theorem 2.3. *(See [18].) There exist bent functions from $\mathbb{F}_2^k$ to $\mathbb{F}_2$ if and only if k is even. Let $k = 2t$ be an even integer. Then the following statements are equivalent.*

(a) *The function f is a bent function.*
(b) *The support of f, $D = f^{-1}(1)$, is a $(2^{2t}, 2^{2t-1} \pm 2^{t-1}, 2^{2t-2} \pm 2^{t-1})$-difference set in $\mathbb{F}_2^{2t}$.*
(c) *The function f_u is balanced for all $u \in \mathbb{F}_2^{2t} \setminus \{0\}$, i.e., $|f_u^{-1}(0)| = |f_u^{-1}(1)|$, where f_u is defined as $f_u(x) = f(x) + f(x + u)$ for all $x \in \mathbb{F}_2^{2t}$.*
(d) *The function $f + g$ is a bent function, where $g : \mathbb{F}_2^{2t} \to \mathbb{F}_2$ is an affine function.*

Maiorana–McFarland bent functions and partial spread ones are the main families of bent functions which have been studied. A Maiorana–McFarland bent function is given by $f(x, y) = x \cdot \sigma(y) + g(y)$, for all $x, y \in \mathbb{F}_2^t$, where $\mathbb{F}_2^{2t}$ is identified with $\mathbb{F}_2^t \times \mathbb{F}_2^t$, σ is an arbitrary permutation of $\mathbb{F}_2^t$, and $g : \mathbb{F}_2^t \to \mathbb{F}_2$ is an arbitrary function. Two subspaces F and G of $\mathbb{F}_2^{2t}$ over $\mathbb{F}_2$ are said to be "*disjoint*" if $F \cap G = \{0\}$. Let $F^* = F \setminus \{0\}$ for any subspace F. A partial spread bent function is given by the following theorem, which is due to Dillon [8].

Theorem 2.4. *(See [8].) Let $f : \mathbb{F}_2^{2t} \to \mathbb{F}_2$ be a function and let $D = f^{-1}(1)$ be the support of f. If $D = \bigcup_{i=1}^{2^{t-1}+1} E_i$ or $D = \bigcup_{i=1}^{2^{t-1}} E_i^*$, then f is a bent function, where all the E_i's are pairwise disjoint t-dimensional subspaces of $\mathbb{F}_2^{2t}$, and $E_i^* = E_i \setminus \{0\}$.*

There are also other constructions of bent functions given by Carlet [4], Dobbertin [10], Hou [12], and others. It is unknown yet whether any of these bent functions are equivalent to Maiorana–McFarland ones or partial spread ones by means of affine linear transforms, complementarity, duality, or some other transforms. For a given bent function f, by Theorem 2.3, we can easily get that $g(x) = f(\sigma(x) + \beta) + \ell(x)$ is also a bent function with $\sigma \in \mathrm{Aut}(\mathbb{F}_2^{2t}, +)$, $\beta \in \mathbb{F}_2^{2t}$, and an affine function $\ell : \mathbb{F}_2^{2t} \to \mathbb{F}_2$. Two such bent functions f and g are called *equivalent*. In this paper, we will consider the problem of how to demonstrate the inequivalence of bent functions.

Let $f : \mathbb{F}_2^{2t} \to \mathbb{F}_2$ be a bent function. The *p-rank* of the function f, denoted by $\mathrm{rank}_p(f)$, is defined to be the p-rank of the difference set $f^{-1}(1)$. It is clear that if there exist $\sigma \in \mathrm{Aut}(\mathbb{F}_2^{2t}, +)$ and $\beta \in \mathbb{F}_2^{2t}$ such that $f(x) = g(\sigma(x) + \beta)$, then the difference sets $f^{-1}(1)$ and $g^{-1}(1)$ are equivalent, from which it follows $\mathrm{rank}_p(f) = \mathrm{rank}_p(g)$. Note that the order of the difference set $f^{-1}(1)$ is $n = 2^{2t-2}$. The p-rank of f is known for any odd prime p by Theorem 2.1. So in this paper we will focus on the 2-ranks of bent functions. It is very difficult to calculate the 2-ranks by using the usual character-theory approach (see [17]). In the remainder of this paper, we use *ranks of bent functions* to mean their 2-ranks, we write $\mathrm{rank}(f)$ for $\mathrm{rank}_2(f)$, and we assume that $t \geqslant 2$.

3. Ranks of bent functions

Let $f : \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function, and let A_f be the $2^k \times 2^k$ matrix whose columns and rows are indexed by elements of $\mathbb{F}_2^k$, and whose (x, y)th entry $A_f(x, y) = f(x + y)$, for all $x, y \in \mathbb{F}_2^k$. The *rank* of the Boolean function f, denoted by $\mathrm{rank}(f)$, is defined to be the rank of the matrix A_f over the field $\mathbb{F}_2$. Note that if f is a bent function, then A_f is just the incidence matrix of the symmetric design associated with the difference set $f^{-1}(1)$. So this definition is the same as that in Section 2 when f is a bent function. Denote by A_f^x the row vector of A_f labeled by the element x, and by C_f the subspace of $\mathbb{F}_2^{2^k}$ generated by the row vectors of the matrix A_f. Then $\mathrm{rank}(f)$ is just the dimension of C_f.

It is clear that $\mathrm{rank}(f) = 0$ or 1 when $f(x) = 0$ or 1, respectively. In the following, we always assume that $\deg(f(x)) \geqslant 1$.

Let $f : \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function. Its polynomial representation in $\mathbb{F}_2[x_1, x_2, \ldots, x_k]/(x_1^2 - x_1, x_2^2 - x_2, \ldots, x_k^2 - x_k)$ can be expressed as

$$f(x_1, x_2, \ldots, x_k) = a_0 + \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k} a_{i_1, i_2, \ldots, i_m} x_{i_1} x_{i_2} \cdots x_{i_m},$$

where a_0 and $a_{i_1, i_2, \ldots, i_m}$'s are 0 or 1. Denote by the boldface letter $\mathbf{f}$ the 2^k dimensional vector whose xth component is $f(x)$. The xth entry in the yth row, i.e., the (x, y)th entry of the matrix A_f can be expressed as

$$A_f^y(x) = A_f(x, y) = f(x + y) = h_0(x) + \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k} h_{i_1, i_2, \ldots, i_m}(x) y_{i_1} y_{i_2} \cdots y_{i_m},$$

where $\deg(h_{i_1, i_2, \ldots, i_m}) \leqslant \deg(f) - m$. Setting $y = 0$, we get that $h_0(x) = f(x)$. Therefore, the yth row of A_f can be expressed as

$$A_f^y = \mathbf{h_0} + \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k} y_{i_1} y_{i_2} \cdots y_{i_m} \mathbf{h_{i_1, i_2, \ldots, i_m}}.$$

Thus, the row vectors of the matrix A_f can be expressed by the vectors $\mathbf{h_0}$ and $\mathbf{h_{i_1,i_2,\ldots,i_m}}$, $1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k$, and the expression matrix is

$$T = \big(\mathbf{j}', \mathbf{x_1}', \ldots, \mathbf{x_k}', (\mathbf{x_1x_2})', \ldots, (\mathbf{x_{k-1}x_k})', (\mathbf{x_1x_2x_3})', \ldots, (\mathbf{x_1x_2}\cdots\mathbf{x_k})'\big),$$

where $\mathbf{j}$ is the vector whose components are all 1. Since the columns of T form a basis of $\mathbb{F}_2^{2^k}$, the matrix T is invertible. Thus C_f can be generated by the vectors $\mathbf{h_0}$ and all those $\mathbf{h_{i_1,i_2,\ldots,i_m}}$ associated with the functions $h_{i_1,i_2,\ldots,i_m}(x)$ in the expression of $A_f^y(x)$.

Lemma 3.1. *Let* $f:\mathbb{F}_2^k \to \mathbb{F}_2$ *be a Boolean function with degree at least* 1. *Then* $\mathbf{j} \in C_f$, $\operatorname{rank}(f) = 2$ *when* $\deg(f) = 1$, *and* $\operatorname{rank}(f) = \operatorname{rank}(f+g)$ *for any Boolean function* $g:\mathbb{F}_2^k \to \mathbb{F}_2$ *with* $\deg(g) \leqslant 1$ *when* $\deg(f) \geqslant 2$.

Proof. When $\deg(f) = 1$, then $\deg(h_{i_1,i_2,\ldots,i_m}) \leqslant 0$. Thus $h_{i_1,i_2,\ldots,i_m}(x) = 0$ or 1. Therefore $C_f = \langle \mathbf{f}, \mathbf{j} \rangle$. So $\operatorname{rank}(f) = 2$.

Now let $\deg(f) = r \geqslant 2$, and let $x_{j_1}x_{j_2}\cdots x_{j_r}$ be a term of $f(x)$ with degree r. Then $h_{j_1,j_2,\ldots,j_r}(x) = 1$, from which it follows $\mathbf{j} \in C_f$. When $g(x) = 1$, then $A^x_{f+g} = A^x_f + \mathbf{j}$ for any row x. Therefore $\operatorname{rank}(f+g) = \operatorname{rank}(f)$. Next for any Boolean function g with $\deg(g) = 1$, we have that $A^y_{f+g}(x) = f(x+y) + g(x+y)$. Let

$$A_f^y(x) = h_0(x) + \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k} h_{i_1,i_2,\ldots,i_m}(x) y_{i_1} y_{i_2} \cdots y_{i_m}$$

and

$$A^y_{f+g}(x) = h'_0(x) + \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k} h'_{i_1,i_2,\ldots,i_m}(x) y_{i_1} y_{i_2} \cdots y_{i_m}.$$

Then $h'_i(x) = h_i(x) + 1$ for some i's with $1 \leqslant i \leqslant k$ and $h'_{i_1,i_2,\ldots,i_m}(x) = h_{i_1,i_2,\ldots,i_m}(x)$ for other coefficients of $y_{i_1}y_{i_2}\cdots y_{i_m}$ in the expressions of $A^y_f(x)$ and $A^y_{f+g}(x)$. Thus $\mathbf{h'_i} = \mathbf{h_i} + \mathbf{j}$, and $\mathbf{h'_{i_1,i_2,\ldots,i_m}} = \mathbf{h'_{i_1,i_2,\ldots,i_m}}$. As $\mathbf{j}$ is in the subspace $\langle \{\mathbf{h_{i_1,i_2,\ldots,i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k\} \rangle$ and in $\langle \{\mathbf{h'_{i_1,i_2,\ldots,i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k\} \rangle$, we have

$$\big\langle \{\mathbf{h_{i_1,i_2,\ldots,i_m}} \mid 1 \leqslant i_1 < \cdots < i_m \leqslant k\} \big\rangle = \big\langle \{\mathbf{h'_{i_1,i_2,\ldots,i_m}} \mid 1 \leqslant i_1 < \cdots < i_m \leqslant k\} \big\rangle.$$

Since $\deg(h_0) = r$ and $\deg(h_{i_1,i_2,\ldots,i_m}) < r$, one can get that $\mathbf{h_0} \notin \langle \{\mathbf{h_{i_1,i_2,\ldots,i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k\} \rangle$. Similarly, $\mathbf{h'_0} \notin \langle \{\mathbf{h'_{i_1,i_2,\ldots,i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k\} \rangle$. Therefore,

$$\operatorname{rank}(f+g) = \operatorname{rank}(f) = 1 + \dim\big(\big\langle \{\mathbf{h_{i_1,i_2,\ldots,i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k\} \big\rangle\big). \qquad \square \quad (3.1)$$

Corollary 3.2. *For any Boolean function* f *with degree at least* 1, *its rank is even.*

Proof. When $\deg(f) = 1$, $\operatorname{rank}(f) = 2$ is even. When $\deg(f) \geqslant 2$, then $\operatorname{rank}(f) = \operatorname{rank}(f+1)$. So without loss of generality, we can assume that $f(0) = 0$. Then the matrix A_f is an alternate matrix over $\mathbb{F}_2$ and its rank is even. $\square$

Corollary 3.3. *Equivalent bent functions have the same rank.*

Proof. Let f and g be equivalent bent functions. That is, $f(x) = g(\sigma(x) + \beta) + \ell(x)$ for some $\sigma \in \mathrm{Aut}(\mathbb{F}_2^{2t}, +)$, $\beta \in \mathbb{F}_2^{2t}$ and a Boolean function $\ell(x)$ with $\deg(\ell) \leqslant 1$. Firstly, $g(x)$ and $g(\sigma(x)+\beta)$ have the same rank because their corresponding difference sets are equivalent. Then by Lemma 3.1, f and g have the same rank. □

Therefore rank is an invariant of bent functions under equivalence. We want to get the inequivalence of bent functions by showing that their ranks are different.

Theorem 3.4. *Let* $f : \mathbb{F}_2^k \to \mathbb{F}_2$ *and* $g : \mathbb{F}_2^s \to \mathbb{F}_2$ *be two Boolean functions with* $\deg(f) \geqslant 1$ *and* $\deg(g) \geqslant 1$, *and define* $w : \mathbb{F}_2^{k+s} \to \mathbb{F}_2$ *by*

$$w(x_1, \ldots, x_k, x_{k+1}, \ldots, x_{k+s}) = f(x_1, \ldots, x_k) + g(x_{k+1}, \ldots, x_{k+s}).$$

Then $\mathrm{rank}(w) = \mathrm{rank}(f) + \mathrm{rank}(g) - 2$.

Proof. Let

$$A_w^y(x) = h_0(x) + \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k+s} h_{i_1, i_2, \ldots, i_m}(x) y_{i_1} y_{i_2} \cdots y_{i_m};$$

$$A_f^y(x) = h_0'(x) + \sum_{1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k} h'_{i_1, i_2, \ldots, i_m}(x) y_{i_1} y_{i_2} \cdots y_{i_m};$$

$$A_g^y(x) = h_0''(x) + \sum_{k+1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k+s} h''_{i_1, i_2, \ldots, i_m}(x) y_{i_1} y_{i_2} \cdots y_{i_m}.$$

By Eq. (3.1),

$$\mathrm{rank}(w) = 1 + \dim\langle \mathbf{h}_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k+s \rangle;$$

$$\mathrm{rank}(f) = 1 + \dim\langle \mathbf{h}'_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k \rangle;$$

$$\mathrm{rank}(g) = 1 + \dim\langle \mathbf{h}''_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid k+1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k+s \rangle.$$

It is clear that $\langle \mathbf{h}_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k+s \rangle = \langle \mathbf{h}'_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k \rangle + \langle \mathbf{h}''_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid k+1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k+s \rangle$ and $\langle \mathbf{h}'_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid 1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k \rangle \cap \langle \mathbf{h}''_{\mathbf{i_1}, \mathbf{i_2}, \ldots, \mathbf{i_m}} \mid k+1 \leqslant i_1 < i_2 < \cdots < i_m \leqslant k+s \rangle = \mathbf{j}$. It follows $\mathrm{rank}(w) = \mathrm{rank}(f) + \mathrm{rank}(g) - 2$. □

Corollary 3.5. *Let* $f : \mathbb{F}_2^k \to \mathbb{F}_2$ *be a Boolean function of degree* r. *Then*

$$\mathrm{rank}(f) \leqslant \sum_{i=0}^{r} \binom{k}{\min\{i, r-i\}}.$$

Proof. When $m \leqslant r/2$, there are at most $\binom{k}{m}$ of $\mathbf{h}_{\mathbf{i_1},\mathbf{i_2},\ldots,\mathbf{i_m}}$ not equal to 0. When $m > r/2$, $\deg(h_{i_1,i_2,\ldots,i_m}) < r/2$. So we have

$$\operatorname{rank}(f) \leqslant \sum_{0\leqslant i\leqslant r/2} \binom{k}{i} + \sum_{r/2<i\leqslant r} \binom{k}{r-i} = \sum_{i=0}^{r} \binom{k}{\min\{i, r-i\}}. \qquad \square$$

It is well known that the lower bound for the 2-rank of any symmetric design on $v = 2^{2t}$ points is $2t+2$ and the case of equality was characterized by Dillon and Schatz [9]. In the following, we will give a new characterization of bent functions whose ranks achieve this lower bound.

Theorem 3.6. *Let t be an integer, and let $f : \mathbb{F}_2^{2t} \to \mathbb{F}_2$ be a bent function. Then* $\operatorname{rank}(f) \geqslant 2t+2$, *with equality if and only if*

$$C_f = \left\{ A_f^x + \beta\mathbf{j}, A_f^x + A_f^0 + \beta\mathbf{j} \;\middle|\; x \in \mathbb{F}_2^{2t},\ \beta \in \mathbb{F}_2 \right\}.$$

Proof. It is clear that $A_f^x + \beta\mathbf{j}, A_f^x + A_f^0 + \beta\mathbf{j} \in C_f$ for any $x \in \mathbb{F}_2^{2t}$ and $\beta \in \mathbb{F}_2$. Now we prove that they are different vectors in C_f. Since f is a bent function, the weight of the vector $A_f^x + \beta\mathbf{j}$ is $2^{2t-1} \pm 2^{t-1}$ for any $x \in \mathbb{F}_2^{2t}$ and $\beta \in \mathbb{F}_2$, but the weight of the vector $A_f^x + A_f^y + \beta\mathbf{j}$ is 2^{2t-1} for any $x \neq y \in \mathbb{F}_2^{2t}$ and $\beta \in \mathbb{F}_2$. Furthermore, $A_f^x + A_f^y + \beta\mathbf{j} \neq 0$, from which it follows that $A_f^x + \beta_1\mathbf{j} \neq A_f^y + \beta_2\mathbf{j}$ for all $x \neq y \in \mathbb{F}_2^{2t}$. Thus $A_f^x + \beta\mathbf{j}$ and $A_f^x + A_f^0 + \beta\mathbf{j}$ are 2^{2t+2} different vectors in C_f, and $\operatorname{rank}(f) = \dim(C_f) \geqslant 2t+2$. $\square$

Let C be a binary linear code of dimension k, and let $\alpha_1, \ldots, \alpha_k$ be a basis of C. Let G be the $k \times n$ matrix whose rows are $\alpha_1, \ldots, \alpha_k$. Then G is called a *generator matrix* of the code C. Let $E = \{\gamma_1, \ldots, \gamma_n\}$ be the multiset containing the columns of G. Then any codeword β_u of C can be written uniquely as $\beta_u = (u \cdot \gamma_1, \ldots, u \cdot \gamma_n)$, for $u \in \mathbb{F}_2^k$.

Lemma 3.7. *Let C be a binary linear $[n,k]$-code, let G be the generator matrix, and let E be the multiset of columns of G. Then every nonzero codeword has the same weight if and only if every nonzero vector in $\mathbb{F}_2^k$ appears the same number of times in the multiset E.*

Proof. If every nonzero vector in $\mathbb{F}_2^k$ appears s times in E, then the weight of the codeword β_u is $s2^{k-1}$ for all $u \in \mathbb{F}_2^k$ with $u \neq 0$. On the other hand, suppose that the vector $u \in \mathbb{F}_2^k$ appears s_u times in E. Without loss of generality, we can assume that $s_0 = 0$. Calculating $\sum_{\alpha\in C} \omega(\alpha)$ and $\sum_{\alpha\in C} \omega(\alpha)^2$ by MacWilliams' formula, we have the following equations:

$$n2^{k-1} = \lambda\left(2^k - 1\right),$$
$$n(n+1)2^{k-2} + B_2 2^{k-1} = \lambda^2\left(2^k - 1\right),$$

where $B_2 = \frac{1}{2}\sum_{u\in\mathbb{F}_2^k}(s_u^2 - s_u)$, $\omega(\alpha) = \lambda$, $\alpha \in C$, $\alpha \neq 0$. Let $n = s(2^k - 1)$, then

$$\sum_{u\in\mathbb{F}_2^k,\, u\neq 0} s_u = s\left(2^k - 1\right),$$

$$\sum_{u\in\mathbb{F}_2^k,\, u\neq 0} s_u^2 = s^2\big(2^k-1\big).$$

It follows that $s_u = s$ for any $u \in \mathbb{F}_2^k$, $u \neq 0$. □

Note that the result in Lemma 3.7 about simplex codes can be found in the book of MacWilliams and Sloane [16].

Theorem 3.8. *Let $f : \mathbb{F}_2^{2t} \to \mathbb{F}_2$ be a Boolean function. Then f is a bent function with* $\operatorname{rank}(f) = 2t+2$ *if and only if there exist two permutations σ, ρ of $\mathbb{F}_2^{2t}$ such that $f(y)+f(x+y)+f(0)+f(x) = \rho(y)\cdot\sigma(x)$, for all $x, y \in \mathbb{F}_2^{2t}$.*

Proof. When f is a bent function with $\operatorname{rank}(f) = 2t+2$, by Theorem 3.6, we know that

$$C_f = \big\{A_f^x + \beta\mathbf{j},\, A_f^x + A_f^0 + \beta\mathbf{j} \,\big|\, x \in \mathbb{F}_2^{2t},\ \beta \in \mathbb{F}_2\big\}.$$

Set

$$C_0 = \big\{A_f^0 + A_f^x + \big(f(0)+f(x)\big)\mathbf{j} \,\big|\, x \in \mathbb{F}_2^{2t}\big\}.$$

Then C_0 is a subspace of C_f with dimension $2t$. It is clear the weight of every nonzero vector in C_0 is 2^{2t-1}. By Lemma 3.7, each nonzero vector in $\mathbb{F}_2^{2t}$ appears a unique time in the columns of the generator matrix of C_0. Therefore there exists a permutation σ of $\mathbb{F}_2^{2t}$ such that $C_0 = \{\alpha_u \mid \alpha_u(x) = u\cdot\sigma(x),\ u, x \in \mathbb{F}_2^{2t}\}$. It follows that

$$\big(A_f^0 + A_f^y + \big(f(0)+f(y)\big)\mathbf{j}\big)(x) = f(y)+f(x+y)+f(0)+f(x) = \rho(y)\cdot\sigma(x),$$

where ρ is another permutation of $\mathbb{F}_2^{2t}$ and $u = \rho(y)$.

On the other hand, suppose that there are two permutations σ and ρ of $\mathbb{F}_2^{2t}$ such that

$$f(y)+f(x+y)+f(0)+f(x) = \rho(y)\cdot\sigma(x),$$

for all $x, y \in \mathbb{F}_2^{2t}$. Let $y = 0$; then $\rho(0) = 0$. So $\rho(y) \neq 0$ for any $y \neq 0$. Furthermore, for any $y \neq 0$,

$$f_y(x) = f(x)+f(x+y) = f(0)+f(y)+\rho(y)\cdot\sigma(x)$$

is a balanced function. So f is a bent function and

$$C_f = \big\{A_f^x + \beta\mathbf{j},\, A_f^x + A_f^0 + \beta\mathbf{j} \,\big|\, x \in \mathbb{F}_2^{2t},\ \beta \in \mathbb{F}_2\big\}.$$

Thus $\operatorname{rank}(f) = 2t+2$. □

At the end of this section, we list the ranks of all bent functions with 6 variables in Table 1 which were found by computer search.

Table 1
Ranks of bent functions $\mathbb{F}_2^6 \to \mathbb{F}_2$

Rank	Number of bent functions
8	241,762,304
12	1,343,913,984
14	3,839,754,240
Total	5,425,430,528

4. Ranks of Maiorana–McFarland bent functions

In this section we will give an upper bound for the ranks of Maiorana–McFarland bent functions. We identify $\mathbb{F}_2^{2t}$ with $\mathbb{F}_2^t \times \mathbb{F}_2^t$. The Maiorana–McFarland bent function is given as $f(x, y) = x \cdot \sigma(y) + g(y)$, for all $x, y \in \mathbb{F}_2^t$, where σ is an arbitrary permutation of $\mathbb{F}_2^t$ and g is a Boolean function $\mathbb{F}_2^t \to \mathbb{F}_2$. Let f be a Maiorana–McFarland bent function. Then A_f is given by $A_f((a, b), (x, y)) = f(a + x, b + y)$. By adding the row $(0, b)$ to the row (a, b), for all $a, b \in \mathbb{F}_2^t$ and $a \neq 0$, and by adding the column $(0, y)$ to the column (x, y), for all $x, y \in \mathbb{F}_2^t$ and $x \neq 0$, we get a matrix B which has the same rank as A_f. The $((a, b), (x, y))$th entry of the matrix B is

$$\begin{cases} f(a+x,b+y)+f(a,b+y)+f(x,b+y)+f(0,b+y)=0, & \text{if } a\neq 0, x\neq 0,\\ f(a,b+y)+f(0,b+y)=a\cdot\sigma(b+y), & \text{if } x=0, a\neq 0,\\ f(x,b+y)+f(0,b+y)=x\cdot\sigma(b+y), & \text{if } a=0, x\neq 0,\\ f(0,b+y)=g(b+y), & \text{if } a=x=0. \end{cases}$$

Let the first 2^t rows and the first 2^t columns of B be indexed as $(0, b)$ and as $(0, y)$, for $b, y \in \mathbb{F}_2^t$. Then the matrix B can be expressed as the following block form

$$\begin{pmatrix} S & T' \\ T & 0 \end{pmatrix},$$

where $S = A_g$ is a $2^t \times 2^t$ matrix, and T is a $(2^{2t} - 2^t) \times 2^t$ matrix, such that

$$S(b, y) = g(b + y), \qquad T\big((a, b), y\big) = a \cdot \sigma(b + y), \quad a \neq 0. \tag{4.1}$$

So we have $2 \cdot \operatorname{rank}(T) \leqslant \operatorname{rank}(f) \leqslant \operatorname{rank}(S\ T') + \operatorname{rank}(T)$. Denote by C_T the subspace of $\mathbb{F}_2^{2^t}$ generated by the row vectors of the matrix T.

Lemma 4.1. *Let $t \geqslant 2$, and let T be the matrix defined in Eq.* (4.1)*. Then $\mathbf{j} \in C_T$, $C_T \subseteq \langle \mathbf{j} \rangle^{\perp}$, and* $\operatorname{rank}(T) \geqslant t + 1$.

Proof. Half the entries of every row of T are 1's and half 0's; so $C_T \subseteq \langle \mathbf{j} \rangle^{\perp}$. Fix a nonzero element $u \in \mathbb{F}_2^t$, and consider the Boolean function $h_u(x) = u \cdot \sigma(x)$. Since the matrix A_{h_u} is a submatrix of T, we have $\mathbf{j} \in C_T$ by Lemma 3.1. Also $\mathbf{h}_u$ is a distinct vector in C_T for each $u \in \mathbb{F}_2^t$, forming a t-dimensional subspace. Since $\mathbf{j}$ is not in this subspace, we have $\operatorname{rank}(T) \geqslant t + 1$. □

By Lemma 4.1, we have again that $\operatorname{rank}(f) \geqslant 2 \cdot \operatorname{rank}(T) \geqslant 2t + 2$ for any Maiorana–McFarland bent function.

Theorem 4.2. *Let $t \geqslant 2$ be an integer, f be a Maiorana–McFarland bent function and let T be the matrix defined in Eq.* (4.1). *Then* $\operatorname{rank}(f) \leqslant 2^t + \operatorname{rank}(T) - 1$. *In particular,* $\operatorname{rank}(f) \leqslant 2^{t+1} - 2$ *with equality if and only if* $\operatorname{rank}(T) = 2^t - 1$.

Proof. We know that $\operatorname{rank}(f) \leqslant \operatorname{rank}(S\ T') + \operatorname{rank}(T)$. When $\operatorname{rank}(S\ T') = 2^t$, then $\mathbf{j} \cdot (S\ T') \neq 0$. We have $\mathbf{j} \cdot S \neq 0$ since $\mathbf{j} \cdot T' = 0$. From $\mathbf{j} \cdot S = |g^{-1}(1)|\mathbf{j}$, we get that $\mathbf{j} \cdot S = \mathbf{j}$. So the rank of the matrix

$$\begin{pmatrix} S & T' \\ \mathbf{j} & 0 \end{pmatrix}$$

is 2^t. Since $\mathbf{j} \in C_T$, we have $\operatorname{rank}(f) \leqslant 2^t + \operatorname{rank}(T) - 1$. □

Of course 6 is the upper bound for any Boolean function of degree at most 2, when $t = 2$, and 14 is the upper bound for any Boolean function of degree at most 3, when $t = 3$. Does there exist a Maiorana–McFarland bent function whose rank meets the upper bounds of Theorem 4.2? Such an example is given in the next theorem.

Let $\mathbb{F}_{2^t}$ be the finite field with 2^t elements. We identity $\mathbb{F}_2^t$ with $\mathbb{F}_{2^t}$ by a bijection $\psi : \mathbb{F}_2^t \to \mathbb{F}_{2^t}$ such that $x \cdot y = \operatorname{Tr}(\psi(x)\psi(y))$, where

$$\operatorname{Tr}(x) = x + x^2 + \cdots + x^{2^{t-1}}$$

is the trace function.

Theorem 4.3. *Let $\sigma(x) = x^{2^t-2}$ and let $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ be an arbitrary Boolean function. Then the rank of the Maiorana–McFarland bent function $f(x, y) = \operatorname{Tr}(x\sigma(y)) + g(y)$ defined by σ and g achieves its upper bound $2^{t+1} - 2$.*

Proof. By Theorem 4.2, we need only to prove that $\operatorname{rank}(T) = 2^t - 1$. Let R be the $2^t \times 2^t$ matrix over $\mathbb{F}_{2^t}$ such that $R(b, x) = \sigma(b + x)$. The xth component of the bth row of R is

$$R^b(x) = (b + x)^{2^t-2} = x^{2^t-2} + b^2 x^{2^t-4} + \cdots + b^{2^t-4} x^2 + b^{2^t-2}.$$

Similarly to the proof of Lemma 3.1, we have

$$\operatorname{rank}(R) = \operatorname{rank}\left(\left\langle \mathbf{x}^{2^t-2}, \mathbf{x}^{2^t-4}, \ldots, \mathbf{x}^2, \mathbf{j} \right\rangle\right) = 2^{t-1}.$$

For any $u \in \mathbb{F}_{2^t}$, let β_i^u be the row vector whose xth component is $\beta_i^u(x) = \operatorname{Tr}(ux^i)$, for $i = 1, \ldots, 2^t - 2$. For each integer $i = 1, \ldots, 2^t - 2$, we choose an integer $r \in \{1, 2, \ldots, t\}$ such that the remainder of $i2^r$ modulo $(2^t - 1)$ is even. We have that $\mathbf{x}^{i2^r}$ can be expressed as a linear combination of the row vectors of R. Therefore,

$$\operatorname{Tr}\left(ux^i\right) = \operatorname{Tr}\left(\left(ux^i\right)^{2^r}\right) = \operatorname{Tr}\left(u^{2^r} \sum v_y \sigma(x + y)\right) = \sum \operatorname{Tr}\left(u^{2^r} v_y \sigma(x + y)\right).$$

So $\beta_i^u \in C_T$. Furthermore,

$$\beta_i^u(x) = \operatorname{Tr}\left(ux^i\right) = ux^i + u^2 x^{i2} + u^{2^2} x^{i2^2} + \cdots + u^{2^{t-1}} x^{i2^{t-1}}.$$

For each i, $1 \leqslant i \leqslant 2^t - 2$, we take $u = 1, v, v^2, \ldots, v^{t-1}$, where v is chosen so that $v, v^2, \ldots, v^{2^{t-1}}$ are all distinct. Then, since the Vandermonde matrix is invertible, we have that the vector $\gamma_i \in C_T$, where the xth component of γ_i is given by $\gamma_i(x) = x^i$, and the code C_T is now taken as the code over $\mathbb{F}_{2^t}$. Obviously $\mathbf{j}, \gamma_1, \ldots, \gamma_{2^t-2}$ are linearly independent; so $\operatorname{rank}(T) = 2^t - 1$. □

We can now contrast the two bent functions $f(x, y) = \operatorname{Tr}(xy) + g_1(y)$ and $h(x, y) = \operatorname{Tr}(xy^{2^t-2}) + g_2(y)$. The first has rank at most $2^t + t$, because the corresponding matrix T has minimum rank $t + 1$, while the second bent function has rank $2^{t+1} - 2$; thus the two are inequivalent when $t > 2$ for any choice of $g_1, g_2 : \mathbb{F}_{2^t} \to \mathbb{F}_2$. In the next section we show that most Desarguesian partial spread bent functions have ranks greater than $2^{t+1} - 2$.

5. Ranks of Desarguesian partial spread bent functions

Another important family of bent functions is the partial spread family which was constructed by Dillon and has been given in Theorem 2.4. This family was seldom discussed because of its complex structure. A special case of the construction in Theorem 2.4 is obtained by identifying $\mathbb{F}_2^{2t}$ with the translation group of an affine translation plane of order $q = 2^t$, whose elements in turn are identified with the points of the plane. The $q/2$ or $q/2 + 1$ t-dimensional subspaces are taken as lines through the origin of the plane. Then a simple inspection of the geometry verifies that we have a bent function. If in fact, the translation plane is the ordinary Desarguesian one $\mathbb{F}_q \times \mathbb{F}_q$, then we have a partial spread bent function, called a *Desarguesian partial spread* (DPS) bent function, which is given in Lemma 5.1.

Lemma 5.1. *Let $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ be a balanced function. Then $f(x, y) = g(xy^{2^t-2})$ is a bent function.*

There are $\binom{16}{8} = 12{,}870$ balanced functions from $\mathbb{F}_{2^4}$ to $\mathbb{F}_2$. We have checked the ranks of all the DPS bent functions from these balanced functions by computer. The results are listed in Table 2.

From the table, we know when $t = 4$ there exist many DPS bent functions (without taking equivalence into account) whose ranks are larger than $30 = 2^{t+1} - 2$, and which are thus not Maiorana–McFarland bent functions. What happens when $t > 4$?

In this section, we identify $\mathbb{F}_2^{2t}$ with $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$, and view the image of a Boolean function as $\{0, 1\} \subset \mathbb{F}_{2^t}$. Let $f : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ be such a function. We write its polynomial representation

Table 2
Ranks of DPS bent functions when $t = 4$

Rank	Number of bent functions
30	270
36	2160
40	1080
42	9360
Total	12,870

in $\mathbb{F}_{2^t}[x, y]/(x^{2^t} - x, y^{2^t} - y)$ as

$$f(x, y) = \sum_{0 \leqslant i, j < 2^t} a_{ij} x^i y^j.$$

Similarly to the case in Section 3, the vector $\mathbf{f}$ is the 2^{2t}-dimensional vector over $\mathbb{F}_{2^t}$ whose (x, y)-component is $\mathbf{f}(x, y) = f(x, y)$. Since $1, x, y, x^2, xy, y^2, \ldots, x^{2^t-1} y^{2^t-1}$ are all the monomial functions, $\mathbf{1}, \mathbf{x}, \mathbf{y}, \mathbf{x^2}, \mathbf{xy}, \mathbf{y^2}, \ldots, \mathbf{x^{2^t-1} y^{2^t-1}}$ is a basis of $\mathbb{F}_{2^t}^{2^{2t}}$. The (x, y)th component of the (a, b)th row of the matrix A_f is

$$A_f^{(a,b)}(x, y) = f(x + a, y + b) = \sum_{0 \leqslant i, j < 2^t} f_{ij}(x, y) a^i b^j,$$

where $\deg(f_{ij}) \leqslant \deg(f) - i - j$. By the same arguments as before, we have the following lemma.

Lemma 5.2. *Let* $f : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ *be a nonzero function. Then* $\operatorname{rank}(f) = \dim(\langle \mathbf{f_{ij}} \mid 0 \leqslant i, j < 2^t \rangle)$, $\mathbf{j} \in \langle \mathbf{f_{ij}} \mid 0 \leqslant i, j < 2^t \rangle$, *and* $\operatorname{rank}(f) = \operatorname{rank}(f + 1)$ *when* $f + 1 \neq 0$.

Since $\operatorname{rank}(f) = \operatorname{rank}(f + 1)$, we always assume that $g(0) = 0$, with $f(x, y) = g(xy^{2^t-2})$. Since any function $g(z)$ can be written as

$$g(z) = \sum_{\alpha \in g^{-1}(1)} \left((z + \alpha)^{2^t-1} + 1\right),$$

we have that $\deg(g) \leqslant 2^t - 2$ if and only if $|g^{-1}(1)|$, the cardinality of the support of g, is even.

Theorem 5.3. *Let* $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ *be any function with* $|g^{-1}(1)|$ *even, and let* $f(x, y) = g(xy^{2^t-2})$. *Then*

$$\operatorname{rank}(f) \leqslant \sum_{r=0}^{t} \binom{t}{r} 2^{\min\{r, t-r\}}.$$

Proof. As $g(0) = 0$, the function g can be written as

$$g(z) = \sum_{i=1}^{2^t-2} \alpha_i z^i.$$

Thus

$$f(x, y) = \sum_{i=1}^{2^t-2} \alpha_i x^i y^{2^t-1-i}$$

is a homogeneous polynomial of degree $2^t - 1$. Therefore

$$f(x+a, y+b) = \sum_{0 \leqslant i,j < 2^t} f_{ij}(x,y) a^i b^j,$$

where

$$f_{ij}(x,y) = \sum_{k=1}^{2^t-2} \alpha_k \binom{k}{i} \binom{2^t - 1 - k}{j} x^{k-i} y^{2^t-1-k-j}.$$

Since f_{ij} is a homogeneous polynomial of degree $2^t - i - j - 1$, we have that the vectors $\mathbf{f_{ij}}$ are linear independent when $i + j$ are different. So

$$\operatorname{rank}(f) = \sum_{n=0}^{2^t-1} \dim\langle \mathbf{f_{ij}} \mid i + j = n \rangle.$$

Set

$$B_{ij} = \left\{ (u,v) \;\middle|\; u+i+v+j = 2^t - 1,\ 1 \leqslant u+i < 2^t - 1,\ \binom{u+i}{i}\binom{v+j}{j} \text{ is odd} \right\}. \quad (5.1)$$

Then

$$f_{ij}(x,y) = \sum_{(u,v) \in B_{ij}} \alpha_{u+i} x^u y^v. \quad (5.2)$$

By Lucas theorem, the binomial coefficient $\binom{m}{k}$ is odd if and only if, when $m = a_0 + a_1 2 + a_2 2^2 + \cdots + a_r 2^r$, and $k = b_0 + b_1 2 + b_2 2^2 + \cdots + b_r 2^r$, for $a_i, b_i = 0, 1$, then $a_i \geqslant b_i$, $0 \leqslant i \leqslant r$. We set

$$\begin{aligned} i &= i_0 + i_1 2 + i_2 2^2 + \cdots + i_{t-1} 2^{t-1}; \\ j &= j_0 + j_1 2 + j_2 2^2 + \cdots + j_{t-1} 2^{t-1}; \\ u &= u_0 + u_1 2 + u_2 2^2 + \cdots + u_{t-1} 2^{t-1}; \\ v &= v_0 + v_1 2 + v_2 2^2 + \cdots + v_{t-1} 2^{t-1}, \end{aligned}$$

where $i_r, j_r, u_r, v_r = 0, 1$, for each $0 \leqslant r < t$. As $\binom{u+i}{i}\binom{v+j}{j}$ is odd, at most one of i_r and u_r is 1, and at most one of j_r and v_r is 1 for each $0 \leqslant r < t$. Since

$$i + j + u + v = 2^t - 1,$$

exactly one of i_r, j_r, u_r and v_r is 1 for each $0 \leqslant r < t$. When $n = i + j = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_r}$ with $0 \leqslant k_1 < k_2 < \cdots < k_r$, there are at most 2^r of (i, j) such that $f_{ij} \neq 0$, so $\dim\langle \mathbf{f_{ij}} \mid i + j = n \rangle \leqslant 2^r$. On the other hand, $2^t - 1 - n = 2^{\ell_1} + 2^{\ell_2} + \cdots + 2^{\ell_{t-r}}$, there are at most

2^{t-r} of $(u, v) \in B_{ij}$, so $\dim\langle \mathbf{f_{ij}} \mid i + j = n\rangle \leqslant \dim\langle \mathbf{x^u y^v} \mid (u, v) \in B_{ij}\rangle = 2^{t-r}$. Furthermore, for a given r, there are $\binom{t}{r}$ of n. Thus

$$\operatorname{rank}(f) \leqslant \sum_{r=0}^{t} \binom{t}{r} 2^{\min\{r,t-r\}}. \qquad \square$$

Firstly we consider a special balanced function $g(z)$ from which a bent function with rank greater than $2^{t+1} - 2$ is derived.

Theorem 5.4. *Let $t \geqslant 4$ be an integer, let $f(x, y) = g(xy^{2^t-2})$, and let*

$$g(z) = \operatorname{Tr}(z) + \sum_{k=1}^{2^t-2} \alpha^{2^t-1-k} z^k,$$

where $\alpha \in \mathbb{F}_{2^t}$ with $\operatorname{Tr}(\alpha) = 1$. When $t = 4$, $\operatorname{rank}(f) = 42$. When $t \geqslant 5$, let $s = [\mathbb{F}_2(\alpha) : \mathbb{F}_2]$ and $d = t/s = [\mathbb{F}_{2^t} : \mathbb{F}_2(\alpha)]$, then $\operatorname{rank}(f) = 2^{t+2} - 4t - 6 - s(d^2 - d)$.

Proof. Let $h(z) = \sum_{k=1}^{2^t-2} \alpha^{2^t-1-k} z^k$. Then

$$h(z) = z^{2^t-1} + (z + \alpha)^{2^t-1} + 1 = \begin{cases} 0, & \text{if } z = 0, \text{ or } \alpha, \\ 1, & \text{otherwise.} \end{cases}$$

So $g(z) = \operatorname{Tr}(z) + h(z)$ is a balanced function. Let $\ell(x, y) = h(xy^{2^t-2})$, $\ell(x + a, y + b) = \sum_{0 \leqslant i,j < 2^t} \ell_{ij}(x, y) a^i b^j$, and let the set B_{ij} be given in Eq. (5.1). Then

$$\ell_{ij}(x, y) = \alpha^j \sum_{k=1}^{2^t-2} \binom{k}{i} \binom{2^t - 1 - k}{j} x^{k-i} (\alpha y)^{2^t-1-k-j} = \alpha^j \sum_{(u,v) \in B_{ij}} x^u (\alpha y)^v.$$

Set $n = i + j$, $P_n(x, y) = \sum_{(u,v) \in B_n} x^u y^v$, where

$$B_n = \left\{ (u, v) \;\middle|\; u + v = 2^t - 1 - n, \ \binom{u + v}{v} \text{ is odd} \right\}.$$

Then

$$\sum_{(u,v) \in B_{ij}} x^u (\alpha y)^v = \begin{cases} P_n(x, \alpha y), & \text{if } i \neq 0,\ j \neq 0, \\ P_n(x, \alpha y) + (\alpha y)^{2^t-n-1}, & \text{if } i = 0,\ j \neq 0, \\ P_n(x, \alpha y) + x^{2^t-n-1}, & \text{if } i \neq 0,\ j = 0, \\ P_n(x, \alpha y) + (\alpha y)^{2^t-n-1} + x^{2^t-n-1}, & \text{if } i = 0,\ j = 0. \end{cases} \tag{5.3}$$

Similarly, let

$$e(x, y) = \operatorname{Tr}\left(xy^{2^t-2}\right) = \sum_{i=2^r,\, 0 \leqslant r < t} x^i y^{2^t-1-i},$$

Table 3
Dimensions of $\langle \mathbf{f_{ij}} \mid i+j=n \rangle$ with $i+j=n$, where $m = 2^t - 1 - n$ and $3 \leqslant r < t-2$

n	$\langle \mathbf{f_{ij}} \mid i+j=n \rangle$	$\dim\langle \mathbf{f_{ij}} \mid i+j=n \rangle$
0	$\langle \mathbf{f} \rangle$	1
2^k	$\left\langle \begin{array}{c} \alpha^{\mathbf{n}}(\mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}) + (\alpha\mathbf{y})^{\mathbf{m}}) + \mathbf{Q_n}(\mathbf{x},\mathbf{y}), \\ \mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}) + \mathbf{x}^{\mathbf{m}} + \mathbf{y}^{\mathbf{m}} \end{array} \right\rangle$	2
$2^{k_1} + 2^{k_2}$	$\left\langle \begin{array}{c} \alpha^{\mathbf{n}}(\mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}) + (\alpha\mathbf{y})^{\mathbf{m}}) + \mathbf{Q_n}(\mathbf{x},\mathbf{y}), \\ \alpha^{\mathbf{2^{k_2}}}\mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}) + \mathbf{y}^{\mathbf{m}}, \\ \alpha^{\mathbf{2^{k_1}}}\mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}) + \mathbf{y}^{\mathbf{m}}, \\ \mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}) + \mathbf{x}^{\mathbf{m}} \end{array} \right\rangle$	$\begin{cases} 3, & \text{if } \alpha^{2^{k_1}-2^{k_2}} = 1, \\ 4, & \text{otherwise.} \end{cases}$
$2^{k_1} + \cdots + 2^{k_r}$	$\langle \mathbf{Q_n}(\mathbf{x},\mathbf{y}), \mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}), \mathbf{y}^{\mathbf{m}}, \mathbf{x}^{\mathbf{m}} \rangle$	4
$2^{k_1} + \cdots + 2^{k_t-2}$	$\langle \mathbf{Q_n}(\mathbf{x},\mathbf{y}), \mathbf{P_n}(\mathbf{x},\alpha\mathbf{y}), \mathbf{y}^{\mathbf{m}}, \mathbf{x}^{\mathbf{m}} \rangle$	$\begin{cases} 3, & \text{if } \alpha^{2^{\ell_1}-2^{\ell_2}} = 1 \text{ and } m = 2^{\ell_1} + 2^{\ell_2}, \\ 4, & \text{otherwise.} \end{cases}$
$2^{k_1} + \cdots + 2^{k_t-1}$	$\langle \mathbf{y}^{\mathbf{m}}, \mathbf{x}^{\mathbf{m}} \rangle$	2
$2^t - 1$	$\langle \mathbf{j} \rangle$	1

and

$$e_{ij}(x,y) = \sum_{(u,v)\in B_{ij},\ u+i=2^r} x^u y^v,$$

where B_{ij} is given in Eq. (5.1). Since $\binom{2^r}{i}$ is odd and $i+u$ is a power of 2, we have $i=0$, or $i=2^r$. If $i=2^r$, then $u=0$, and $e_{ij} = y^{2^t-i-j-1}$. So we have

$$e_{ij}(x,y) = \begin{cases} Q_n(x,y), & \text{if } i=0, \\ y^{2^t-n-1}, & \text{if } i=2^r \text{ and } \binom{n}{i} \text{ is odd}, \\ 0, & \text{otherwise}, \end{cases} \tag{5.4}$$

where

$$Q_n(x,y) = \sum_{0\leqslant r<t,\ \binom{2^t-1-2^r}{n} \text{ is odd}} x^{2^r} y^{2^t-1-2^r-n}.$$

Since $f_{ij} = \ell_{ij} + e_{ij}$, we see that the explicit vectors collected in Table 3 form a sorted spanning set for the code of f.

When $t \geqslant 5$, we have that

$$\operatorname{rank}(f) = \sum_{n=0}^{2^t-1} \dim\langle \mathbf{f_{ij}} \mid i+j=n \rangle = 2^{t+2} - 4t - 6 - 2e,$$

where e is the number of pairs (u,v) such that $0 \leqslant u < v < t$ and $\alpha^{2^v-2^u} = 1$. It is clear that $e = s(d^2-d)/2$. So we have that

$$\operatorname{rank}(f) = 2^{t+2} - 4t - 6 - s\big(d^2-d\big).$$

When $s = 1$ and $d = t$, $s(d^2 - d)$ reaches its maximum value $t^2 - t$ while $s = t$ and $d = 1$, $s(d^2 - d)$ reaches its minimal value 0. It follows that

$$2^{t+2} - t^2 - 3t - 6 \leqslant \mathrm{rank}(f) \leqslant 2^{t+2} - 4t - 6.$$

Furthermore, $\mathrm{rank}(f) = 2^{t+2} - 4t - 6$ if and only if $s = t$, and $\mathrm{rank}(f) = 2^{t+2} - t^2 - 3t - 6$ if and only if $\alpha = 1$ and t is odd.

Similarly, when $t = 4$, we have that

$$\mathrm{rank}(f) = \sum_{n=0}^{2^4-1} \dim\langle \mathbf{f_{ij}} \mid i + j = n\rangle = 2^{4+2} - 4 \cdot 4 - 6 - e = 42 - e,$$

where $e = s(d^2 - d)/2$ as before. Since $\mathrm{Tr}(\alpha) = d(\alpha + \alpha^2 + \cdots + \alpha^{2^{s-1}}) = 1$, we know that d is odd. But d is a divisor of 4. Therefore $d = 1$ and $e = 0$. Thus $\mathrm{rank}(f) = 42$. □

In the following, we consider a general nonzero function g, not necessarily balanced. We assume that $|g^{-1}(1)|$ is even and $g(0) = 0$. Then the function g can be written as

$$g(z) = \sum_{\alpha \in g^{-1}(1)} \left((z + \alpha)^{2^t-1} + 1\right) = \sum_{\alpha \in g^{-1}(1)} \left(z^{2^t-1} + (z + \alpha)^{2^t-1} + 1\right).$$

Let $f(x, y) = g(xy^{2^t-2})$ and again let

$$f(x + a, y + b) = \sum_{0 \leqslant i,j < 2^t} f_{ij}(x, y) a^i b^j.$$

Then

$$f_{ij}(x, y) = \sum_{\alpha \in g^{-1}(1)} \alpha^j P_n(x, \alpha y) = \sum_{(u,v) \in B_n} \left(\sum_{\alpha \in g^{-1}(1)} \alpha^{j+v} \right) x^u y^v,$$

where $P_n(x, y)$ and B_n are given in the proof of Theorem 5.4. Thus

$$\dim\langle \mathbf{f_{ij}} \mid i + j = n\rangle = \mathrm{rank}(H_n), \tag{5.5}$$

where $n = 2^{k_1} + \cdots + 2^{k_r}$, H_n is the $2^r \times 2^{t-r}$ matrix over $\mathbb{F}_{2^t}$ whose rows are indexed by integers j such that the binomial coefficient $\binom{n}{j}$ is odd and whose columns are indexed by integers v such that the binomial coefficient $\binom{2^t-1-n}{v}$ is odd, and whose (j, v)th entry $H_n(j, v) = \sum_{\alpha \in g^{-1}(1)} \alpha^{j+v}$.

Firstly we give the following lemma.

Lemma 5.5. *Let K be a field of characteristic p. If the elements $a_1, a_2, \ldots, a_n$ of K satisfy*

$$S_j = \sum_{i=1}^{n} a_i^j = 0,$$

for $j = 0, 1, \ldots, n-1$, then every $a \in K$ will appear pm_a times in the multiset $\{a_1, a_2, \ldots, a_n\}$ for some integer m_a.

Proof. The result is similar to the Newton formula in a field of characteristic 0. Let $\{a_1, a_2, \ldots, a_n\} = \{b_1, b_2, \ldots, b_k\}$ where b_i, $1 \leqslant i \leqslant k$, are different elements in K. Let $\beta_i = (1, b_i, b_i^2, \ldots, b_i^{k-1})'$. Since

$$\det(\beta_1, \beta_2, \ldots, \beta_k) = \prod_{1 \leqslant i < j \leqslant k} (b_j - b_i) \neq 0,$$

we have $p \mid q_i$ from $\sum_{i=1}^{k} q_i \beta_i = 0$, where b_i appears q_i times in $\{a_1, a_2, \ldots, a_n\}$. □

Theorem 5.6. *Let $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ be a nonzero function, let $|g^{-1}(1)|$ be even, $g(0) = 0$, and let $f(x, y) = g(xy^{2^t-2})$ be a function from $\mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ to $\mathbb{F}_2$. Then* $\operatorname{rank}(f) \geqslant 2^{t+1} - 2$.

Proof. From the discussions above, we have that

$$\operatorname{rank}(f) = \sum_{n=0}^{2^t-1} \dim\langle \mathbf{f_{ij}} \mid i + j = n \rangle = \sum_{n=0}^{2^t-1} \operatorname{rank}(H_n).$$

Let $S_k = \sum_{\alpha \in g^{-1}(1)} \alpha^k$. Then the entries of the matrix H_n are just those S_k's for $k = 0, 1, \ldots, 2^t - 1$. So $\operatorname{rank}(H_n) \geqslant 1$. It is clear that $\operatorname{rank}(H_n) = 1$ for $n = 0$ and $n = 2^t - 1$. Now suppose that there is some other n, $1 \leqslant n \leqslant 2^t - 2$, with $\operatorname{rank}(H_n) = 1$. Without loss of generality, we can assume that n is odd because the transpose of the matrix H_n is just the matrix H_{2^t-1-n}. Since the concatenation of the odd rows of H_n is the first row of H_1 and that of the even rows of H_n is the second row of H_1, we have $\operatorname{rank}(H_1) = 1$. Denote by γ_1 and γ_2 the two rows of H_1. Then $\gamma_1 = b\gamma_2$ for some $b \in \mathbb{F}_{2^t}$, $b \neq 0$. A simple calculation tells us that $S_{2^{s_1}+\cdots+2^{s_k}}^{2^r} = S_{2^{s_1+r}+\cdots+2^{s_k+r}}$ and $S_0 = S_{2^t-1} = 0$. Therefore $S_{2^r} = S_1^{2^r} = (bS_0)^{2^r} = 0$. It follows $S_{2^s+2^r} = S_{2^{s-r}+1}^{2^r} = (bS_{2^{s-r}})^{2^r} = 0$. Doing the same procedure, we get that $S_k = 0$ for $k = 0, 1, \ldots, 2^t - 1$, a contradiction. Therefore $\operatorname{rank}(H_n) \geqslant 2$ for $n = 1, 2, \ldots, 2^t - 2$, from which it follows

$$\operatorname{rank}(f) = \sum_{n=0}^{2^t-1} \operatorname{rank}(H_n) \geqslant 2 + 2\left(2^t - 2\right) = 2^{t+1} - 2. \qquad \square$$

Corollary 5.7. *Let $f(x, y) = g(xy^{2^t-2})$ be a bent function, where $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ is a balanced function. Then* $\operatorname{rank}(f) \geqslant 2^{t+1} - 2$.

From the proof of Theorem 5.6, we know that $\operatorname{rank}(f) = 2^{t+1} - 2$ if and only if $\operatorname{rank}(H_n) = 2$ for all $0 < n < 2^t - 1$, which is a very strict condition for a balanced function g when $t \geqslant 4$. In the following, we will prove that the rank of almost every DPS bent function cannot reach its lower bound $2^{t+1} - 2$. Therefore almost every DPS bent function is inequivalent to any Maiorana–McFarland bent function.

Now let $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ be a nonzero function, let $|g^{-1}(1)|$ be even, and $g(0) = 0$ as in Theorem 5.6. Set $g^{-1}(1) = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $n = 2^{s_1} + 2^{s_2} + \cdots + 2^{s_r}$, where $0 \leqslant s_1 < s_2 <$

$\cdots < s_r < t$. Let G_n be the $2^r \times m$ matrix, whose rows are indexed by the integer i such that $\binom{n}{i}$ is odd and columns are indexed by the integer j with $1 \leqslant j \leqslant m$, and whose (i, j)th entry $G_n(i, j) = \alpha_j^i$. It is clear that

$$H_n = G_n G'_{2^t-1-n}.$$

Lemma 5.8. *Let m be an even integer with $2^{k-1} < m \leqslant 2^k$, and let $n = 2^s(2^k - 1)$ for some integer s, $0 \leqslant s \leqslant t - k$. Then for any m-subset $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ of $\mathbb{F}_{2^t}$, we have* $\operatorname{rank}(G_n) = m$.

Proof. The result follows immediately by noting that the determinant of the first m rows of G_n is the Vandermonde type. □

Lemma 5.9. *Let m be a given even integer with $2^{k-1} < m \leqslant 2^k$, and let μ_t be the number of integers n, $0 \leqslant n < 2^t$, such that for any s, $0 \leqslant s \leqslant t - k$, $\binom{n}{2^s(2^k-1)}$ is not odd. Then* $\lim_{t\to\infty} \frac{\mu_t}{2^t} = 0$.

Proof. It is clear that μ_t is just the number of n such that there is no consecutive k 1's in the binary representation of n. So we have the following recurrence relation

$$\mu_t = \mu_{t-1} + \mu_{t-2} + \cdots + \mu_{t-k}, \quad t \geqslant k,$$

with the initial conditions $\mu_i = 2^i$, $0 \leqslant i \leqslant k - 1$. The modulus of every root of its characteristic equation is less than 2, from which it follows that $\lim_{t\to\infty} \frac{\mu_t}{2^t} = 0$. □

Theorem 5.10. *For any given even integer m with $2^{k-1} < m \leqslant 2^k$. Let $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ be a nonzero function, $|g^{-1}(1)| = m$, $g(0) = 0$, and let $f(x, y) = g(xy^{2^t-2})$. Then for any $c < m$,*

$$\operatorname{rank}(f) > c \cdot 2^t,$$

for sufficiently large t.

Proof. If there exist s_1, s_2 such that $\binom{n}{2^{s_1}(2^k-1)}$ and $\binom{2^t-1-n}{2^{s_2}(2^k-1)}$ are odd. Then $G_{2^{s_1}(2^k-1)} G'_{2^{s_2}(2^k-1)}$ is a submatrix of H_n with rank m. So we have

$$\operatorname{rank}(f) = \sum_{n=0}^{2^t-1} \operatorname{rank}(H_n) > m\left(2^t - 2\mu_t\right) \geqslant c \cdot 2^t. \qquad \square$$

Now consider balanced functions in order to deal with DPS bent functions. For convenience, we say a balanced function $g : \mathbb{F}_{2^t} \to \mathbb{F}_2$ is *minimal* if the rank of its corresponding DPS bent function $f(x, y) = g(xy^{2^t-2})$ achieves the lower bound $2^{t+1} - 2$ and $g(0) = 0$. Let $\mathcal{G}$ (respectively $\tilde{\mathcal{G}}$) be the set of all balanced (respectively minimal balanced) functions from $\mathbb{F}_{2^t}$ to $\mathbb{F}_2$ with $g(0) = 0$. For any $g_1, g_2 \in \mathcal{G}$, denote by $\mathrm{d}(g_1, g_2)$ the Hamming *distance* between g_1 and g_2, which is defined to be $|(g_1 + g_2)^{-1}(1)|$, the cardinality of the support of $g_1 + g_2$. It is clear that $\mathrm{d}(g_1, g_2)$ is even since

$$\mathrm{d}(g_1, g_2) = \left|g_1^{-1}(1) \cap g_2^{-1}(0)\right| + \left|g_1^{-1}(0) \cap g_2^{-1}(1)\right| = 2^t - 2\left|g_1^{-1}(1) \cap g_2^{-1}(1)\right|.$$

Let M be a given integer with $M \geqslant 12$ and $4 \mid M$, and let $f_i(x, y) = g_i(xy^{2^t-2})$, $i = 1, 2$. For a sufficiently large t, if $\mathrm{d}(g_1, g_2) = m$ with $6 \leqslant m \leqslant M$, then

$$\mathrm{rank}(f_1) + \mathrm{rank}(f_2) \geqslant \mathrm{rank}(f_1 + f_2) > 4 \cdot 2^t = 2^{t+2}$$

by Theorem 5.10. So at most one of the DPS bent functions f_1 and f_2 is minimal. Therefore for any $\tilde{g}_1, \tilde{g}_2 \in \tilde{\mathcal{G}}$, we have that $\mathrm{d}(\tilde{g}_1, \tilde{g}_2) \leqslant 4$ or $\mathrm{d}(\tilde{g}_1, \tilde{g}_2) > M$. Let $\mathcal{G}'$ be a maximum subset of $\tilde{\mathcal{G}}$ such that $\mathrm{d}(g'_1, g'_2) > M$ for any $g'_1, g'_2 \in \mathcal{G}'$. For any $\tilde{g} \in \tilde{\mathcal{G}}$, there are at most $\sum_{i=0}^{2} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i}$ elements $\tilde{h} \in \tilde{\mathcal{G}}$ with $\mathrm{d}(\tilde{g}, \tilde{h}) \leqslant 4$. Thus it is clear that

$$|\mathcal{G}'| \geqslant \frac{|\tilde{\mathcal{G}}|}{\sum_{i=0}^{2} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i}}.$$

For any $g' \in \mathcal{G}'$, let

$$\mathcal{B}_{g'} = \big\{ g \in \mathcal{G} \;\big|\; \mathrm{d}(g, g') \leqslant M/2 \big\}.$$

It is clear that $|\mathcal{B}_{g'}| = \sum_{i=0}^{M/4} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i}$ for any $g' \in \mathcal{G}'$, and $\mathcal{B}_{g'_1} \cap \mathcal{B}_{g'_2} = \emptyset$ for any distinct $g'_1, g'_2 \in \mathcal{G}'$. From $\mathcal{G} \supseteq \bigcup_{g' \in \mathcal{G}'} \mathcal{B}_{g'}$, we have

$$|\mathcal{G}| \geqslant |\mathcal{G}'| \sum_{i=0}^{M/4} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i} \geqslant \frac{|\tilde{\mathcal{G}}|}{\sum_{i=0}^{2} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i}} \sum_{i=0}^{M/4} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i}.$$

So

$$\frac{|\tilde{\mathcal{G}}|}{|\mathcal{G}|} \leqslant \frac{\sum_{i=0}^{2} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i}}{\sum_{i=0}^{M/4} \binom{2^{t-1}}{i}\binom{2^{t-1}-1}{i}},$$

from which the following theorem is proved.

Theorem 5.11. *Let $\mathcal{G}$ (respectively $\tilde{\mathcal{G}}$) be the set of all balanced (respectively minimal balanced) functions from $\mathbb{F}_{2^t}$ to $\mathbb{F}_2$ with $g(0) = 0$. Then $\lim_{t\to\infty} \frac{|\tilde{\mathcal{G}}|}{|\mathcal{G}|} = 0$. Therefore, the rank of almost every DPS bent functions cannot reach its lower bound.*

Similarly, we can prove that for any given integer c, the probability of DPS bent functions having ranks less than $c \cdot 2^t$ approaches zero as t increases.

At the end of this section, consider the upper bound for the ranks of DPS bent functions in Theorem 5.3. Theorem 5.4 tells us that this bound is tight when $t = 4$ or 5. When $t = 6$, there do exist bent functions whose ranks achieve this upper bound 306. An example is given by the following balanced function g whose support is

$$g^{-1}(1) = \big\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^{13}, \alpha^{14}, \alpha^{15}, \alpha^{16}, \alpha^{17}, \alpha^{22}, \alpha^{23}, \alpha^{26}, \alpha^{27}, \alpha^{31}, \alpha^{32},$$
$$\alpha^{33}, \alpha^{37}, \alpha^{43}, \alpha^{44}, \alpha^{46}, \alpha^{53}, \alpha^{54}, \alpha^{55}, \alpha^{56}, \alpha^{58}, \alpha^{59}, \alpha^{60}, \alpha^{61}, \alpha^{62}\big\},$$

where α is a primitive element of $\mathbb{F}_{64}$ with $\alpha^6 + \alpha^5 + 1 = 0$.

Table 4
Bounds of ranks of some bent functions

Type	Lower bound	Upper bound
All bent functions	$2t+2$	$\sum_{k=0}^{t}\binom{2t}{\min\{k,t-k\}}$ (tight when $t \leqslant 4$)
Maiorana–McFarland	$2t+2$	$2^{t+1}-2$
Desarguesian partial spread	$2^{t+1}-2$	$\sum_{r=0}^{t}\binom{t}{r}2^{\min\{r,t-r\}}$(tight when $t \leqslant 6$)

6. Conclusion and discussion

In this paper we define the rank of a bent function and prove some upper and lower bounds for the rank. Some examples of bent functions which meet those bounds are also given. As a consequence, we can prove the inequivalence of some bent functions. The bounds of the ranks of some bent functions are listed in Table 4.

From Section 5, there do exist bent functions whose ranks are larger than $2^{t+2}-4$ for sufficiently large t. Now let $f:\mathbb{F}_2^{2t}\to\mathbb{F}_2$ be a bent function such that $\operatorname{rank}(f) > 2^{t+2}-4$. Define the function $g:\mathbb{F}_2^{2t+2}\to\mathbb{F}_2$ by

$$g(x_1,\ldots,x_{2t+2}) = f(x_1,\ldots,x_{2t}) + x_{2t+1}x_{2t+2}.$$

Then g is also a bent function whose rank

$$\operatorname{rank}(g) = \operatorname{rank}(f) + 2 > 2^{t+2} - 2.$$

So g is inequivalent to any Maiorana–McFarland bent function and $\deg(g) \leqslant t$. Also it is clear that bent functions with different degrees are not equivalent. Thus g is inequivalent to any DPS bent function since the degree of a DPS bent function is exactly half the dimension of the space. Furthermore, from Corollary 6.2 below, we can say that g is inequivalent to most partial spread bent functions by checking their degrees. The following lemma can be gotten easily from Theorem 14 of [16, Chapter 13].

Lemma 6.1. *Let $f:\mathbb{F}_2^k\to\mathbb{F}_2$ be a Boolean function with $\deg(f)\leqslant r$. Then $\deg(f)=r$ if and only if there exists an r-dimensional subspace H of $\mathbb{F}_2^k$ such that $|H\cap f^{-1}(1)|$ is odd.*

Corollary 6.2. *Let $f:\mathbb{F}_2^{2t}\to\mathbb{F}_2$ be a partial spread bent function. Then $\deg(f)=t$ if one of the following statements is satisfied, where all the E_i's are pairwise disjoint t-dimensional subspaces of $\mathbb{F}_2^{2t}$, and $E_i^* = E_i\setminus\{0\}$.*

(a) $f^{-1}(1) = \bigcup_{i=1}^{2^{t-1}} E_i^*$.
(b) $f^{-1}(1) = \bigcup_{i=1}^{2^{t-1}+1} E_i$ *and there exists another t-dimensional subspace H such that* $H\cap f^{-1}(1)=\{0\}$.

Acknowledgments

The authors would like to thank Qing Xiang, Ulrich Dempwolff, and Gregor Leander for many valuable discussions. They would also like to express their gratitude to the referees for valuable comments and constructive suggestions on the manuscript.

References

[1] K.T. Arasu, A new family of cyclic difference sets with Singer parameters in characteristic three, Des. Codes Cryptogr. 28 (2003) 75–91.
[2] E.F. Assmus Jr., J.D. Key, Designs and Their Codes, Cambridge Univ. Press, Cambridge, 1992.
[3] T. Beth, D. Jungnickel, H. Lenz, Design Theory, vol. I, second ed., Encyclopedia Math. Appl., vol. 78, Cambridge Univ. Press, Cambridge, 1999.
[4] C. Carlet, A construction of bent functions, in: Finite Fields and Applications, in: London Math. Soc. Lecture Note, vol. 233, Cambridge Univ. Press, Cambridge, 1996, pp. 47–58.
[5] D.B. Chandler, Q. Xiang, The invariant factors of some cyclic difference sets, J. Combin. Theory Ser. A 101 (2003) 131–146.
[6] D.B. Chandler, Q. Xiang, Cyclic relative difference sets and their p-rank, Des. Codes Cryptogr. 30 (2003) 325–343.
[7] U. Dempwolff, Automorphisms and equivalence of bent functions and of difference sets in elementary abelian 2-groups, Comm. Algebra 34 (2006) 1077–1131.
[8] J.F. Dillon, Elementary Hadamard difference sets, PhD thesis, University of Maryland, 1974.
[9] J.F. Dillon, J.R. Schatz, Block designs with the symmetric difference property, in: R.L. Ward (Ed.), Proc. NSA Mathematical Sciences Meetings, U.S. Government Printing Office, Washington, DC, 1987, pp. 159–164.
[10] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in: Fast Software Encryption–FSE'94, in: Lecture Notes in Comput. Sci., vol. 1008, Springer, Berlin, 1995, pp. 61–74.
[11] H. Dobbertin, G. Leander, A survey of some recent results on bent functions, in: T. Helleseth, et al. (Eds.), SETA 2004, in: Lecture Notes in Comput. Sci., vol. 3486, Springer, Berlin, 2005, pp. 1–29.
[12] X. Hou, Results on bent functions, J. Combin. Theory Ser. A 80 (1997) 232–246.
[13] X. Hou, Cubic bent functions, Discrete Math. 189 (1998) 149–161.
[14] M. Klemm, Über den p-Rang von Inzidenzmatrizen, J. Combin. Theory Ser. A 43 (1986) 138–139.
[15] E. Lander, Symmetric Design: An Algebraic Approach, London Math. Soc. Lecture Note, vol. 74, Cambridge Univ. Press, Cambridge, 1983.
[16] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.
[17] A. Pott, Finite Geometry and Character Theory, Lecture Notes in Math., vol. 1601, Springer, Berlin, 1995.
[18] J. Wolfmann, Bent functions and coding theory, in: A. Pott, et al. (Eds.), Difference Sets, Sequences and Their Correlation Properties, Kluwer Academic, 1999, pp. 393–418.